Cost Estimation for Secure Software & Systems
Workshop Introduction

Edward Colbert, Sr. Research Associate
Dr. Barry Boehm, Director
Center for System & Software Engineering
{ecolbert, boehm}@csse.usc.edu
http://csse.usc.edu

Ground Station Architecture Workshop (GSA)
Goal Of Presentation

- Review Research
  - Draft model for early costing of system security
  - Extensions to COCOMO II for development of secure software systems ("COSECMO")

- Invite
  - Expert opinion
  - Data (Collection)
U.S. Federal Aviation Administration Needs

- U.S. Congressional & Congressional Office of Management & Budget (OMB) requires each U.S. agency to **plan & budget for security** throughout life–cycle of system

- July ’03, FAA CTO asked USC CSSE to research cost estimation for secure systems
  - Completing 3rd phase
Estimating Cost for Secure Software–Intensive Systems

- Widely held that engineering security will substantially raise software–project cost

- Wide variation in amount of added cost estimated by different models
  - e.g.
    - [Bisignani and Reed 1988] estimates engineering highly–secure software will increase costs by \textit{factor of 8}
    - 1990’s Softcost-R model estimates \textit{factor of 3.43} [Reifer 2002]

- Models based on 1985 “Orange Book”
Estimating Software Cost

- 1981 *Constructive Cost Model (COCOMO)*
  - 80 projects
  - Developed by Dr. Barry Boehm

- 2000 COCOMO II
  - 160+ projects
    - (now about 200 in database)
  - Authors
    - Dr. Boehm (USC CSSE)
    - A. Winsor Brown (USC CSSE)
    - Dr. Chris Abts (Univ. of Texas)*
    - Dr. Sunita Chulani (IBM)*
    - Dr. Brad Clark (Software Metrics, Inc.)*
    - Dr. Elis Horowitz (USC CSSE)
    - Dr. Ray Madachy (CostPlus, USC CSSE)*
    - Don Reifer (Reifer Consultants, Inc.)
    - Dr. Bert Steece (USC Marshall School of Business)
  - * Dr. Boehm’s Ph.D. Student

- COCOMO I/II is basis of many commercial products

- Dr. Barry Boehm
  - Director, USC Center for Software Engineering (USC CSSE)
  - Author of *Software Engineering Economics*
    - Seminal work on topic
  - Lead author of *Software Cost Estimation and COCOMO II*
  - Creator of *Spiral Model*
  - Former Director of Defense Advanced Research Product Agency (DARPA) Information Science & Technology Office
COCOMO II & Security

Software size estimate

Effort Multipliers (EM): Software product, process, project & personnel cost drivers

Project Scale Factors (SF): maturity, risk, flexibility, teamwork & precedededness

Software organization’s project data

COCOMO II Model

Effort & duration estimates

Cost, schedule distribution by phase, activity, increment

COCOMO II recalibrated to organization’s data

Effort in Person Month

\[ E_{\text{base-estimate}} = A \times (\text{Size})^S \times \Pi(EM_i) \]

\[ S = B + 0.01 \times \Sigma(SF_i) \]
COCOMO II Modeling Methodology

- Analyzed
  - Published industry practices with respect to security
    inc. standards like Common Criteria
  - 149 Security Targets registered on National Information Assurance Partnership (NIAP) Website
    - SAR’s & FAR Usage
      - Overall
      - By
        » Project Domain
        » Life-cycle phase
        » Security goals
        » COCOMO driver

- Conducted preliminary surveys of experts in SW development & in security
COCOMO Estimation with Security

\[
\%\text{Effort}(EAL) = \%\text{Effort}_3 \times SECU^{(EAL - 3)} \quad \text{for} \quad EAL \geq 3
\]
\[
= 0 \quad \text{for} \quad EAL < 3
\]

\[
\text{Effort(Internal Assurance)} = \text{Effort(Base)} \times \%\text{Effort}(EAL)
\]

\[
\text{Effort(Total)} = \text{Effort(Base)} + \text{Effort(Internal Assurance)} + \text{Effort(Independent Assurance)}
\]

where:

- **SECU** — Calibration constant
- **EAL** — Evaluated Assurance Level or (Equivalent)
- **Effort(Base)** — Result from basic COCOMO II formula
- **Effort(Internal Assurance)** — Effort of developer to verify that security requirements are met
- **\%\text{Effort}_3** — Percent add effort at level 3 (see table next page)
- **\%\text{Added Effort}** — Percent added effort for desired AL
- **Effort(Independent Assurance)** — Effort of independent organization’s effort to verify that security requirements are met.
COCOMO Estimation with Security (cont.)

%Added Effort when SECU = 2.5

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>0</td>
<td>20</td>
<td>50</td>
<td>125</td>
<td>312</td>
<td>781</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>0</td>
<td>40</td>
<td>100</td>
<td>250</td>
<td>625</td>
<td>1560</td>
<td></td>
</tr>
<tr>
<td>100</td>
<td>0</td>
<td>60</td>
<td>150</td>
<td>375</td>
<td>937</td>
<td>2344</td>
<td></td>
</tr>
<tr>
<td>1000</td>
<td>0</td>
<td>80</td>
<td>200</td>
<td>500</td>
<td>1250</td>
<td>3125</td>
<td></td>
</tr>
</tbody>
</table>

- Level names are COCOMO standard + 2
  - Mapping currently from Common Criteria v2
    - Nominal=1 or 2, High=3, Ultra=7
    - For 3+, Reliability = Very-High
  - Working on other mappings (e.g. NIST 800-52, DoD 8500, Orange Book)
- Values are based on survey of small group of experts
- Published data points fit reasonably
  - Only a few data points
COCOMO Estimation with Security (cont.)

%Added Effort

What’s your opinion?
Example of COCOMO Estimation with Security

Assume:

- Reliability = Very-High
- All other drivers = Nominal
- Trusted SW = 5 KSLOC

If Assurance = Nominal (EAL 1 or 2)

Effort (Total) = 21.75 person-months

If Assurance = Very-High (EAL 4)

Effort (Internal Assurance) = 21.75 * 50% = 10.88 person-months
Effort (Total) = 21.75 + 10.88 = 32.63 person-months

If Assurance = Ultra-High (EAL 7)

Effort (Internal Assurance) = 21.75 * 780% = 169.62 person-months
Effort (Total) = 21.75 + 10.88 = 191.37 person-months
Formula for Cost of System & Security

\[ C_{\text{total}} = C_{\text{Initial/Mission Analysis}} + C_{\text{Investment Analysis}} + C_{\text{System Engineering}} + C_{\text{Dev & Imp}} + C_{\text{Sys of Sys Integration}} + C_{\text{Install/Deployment}} + C_{\text{O&M}} + C_{\text{Disposal}} \]

\[ C_{\text{Dev & Imp}} = C_{\text{Design & Build HW}} + C_{\text{Design & Build SW}} + C_{\text{Purchased Services}} + C_{\text{COTS-Sys}} + C_{\text{Env-Mods-design}} + C_{\text{Bus-Proc-Re-engineering}} \]

\[ C_{\text{total (Security)}} = C_{\text{total (with security)}} - C_{\text{total (without security)}} \]

\[ C = \text{Cost} \]
Cost Model for Secure System Approach

- Analyzed Work-breakdown Structure (WBS)
  - Identified activities affected by Security

- Identified major sources of cost
  - To develop & own system
  - Including: facilities, equipment, people, acquired systems, services

- Determine approaches to estimate cost for each source of cost
  - Activity–based (e.g. Labor hours)
  - Unit costing (e.g. # firewalls)
  - Analogy-based (e.g. It cost us $XXX last year,…)
  - Parametric (e.g. COCOMO II estimate)
Developed Prototype Tool Support

- COSECMO Prototype in COINCOMO

- 4th Prototype Tool Screenshot#1
  Total from Cost Sources

Current COCOMO II Cost Drivers

Security Assurance Level
To Do

- Get more feedback from security community
- Refine models
- Refine costing prototypes
- Refine Delphi
- Collect & analyze data
- Write papers & Ph.D. thesis (theses?)
Next Costing Secure Systems Workshop

- Date: TBD June
  - Also, workshop at fall COCOMO Forum
- Location: University of Southern California, LA
- Cost:
  - TBD (nominal)
In Case You Aren’t Sure That Security Is Important

I think there’s a spy among us...
References


